IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

Angeline Hudson, on behalf of herself and all others similarly situated, Plaintiff, v. HCA Inc. and HCA Healthcare, Inc., Defendants.	)	Case No. **CLASS ACTION COMPLAINT**

Plaintiff Angeline Hudson ("Plaintiff"), by her undersigned counsel, files this Class Action Complaint on behalf of herself and a class of all similarly situated persons against Defendants HCA Inc. and HCA Healthcare, Inc. (together, "HCA" or "Defendants"). Plaintiff bases the forgoing allegations upon personal information and belief, the investigation of counsel, and state the following:

INTRODUCTION

1. Plaintiff brings this class action complaint on behalf of a class of persons impacted by HCA's failure to safeguard, monitor, maintain, and protect highly sensitive Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (together, "Sensitive Information"). HCA collected, stored, and maintained Plaintiff's and the Class's Sensitive Information as part of its business activities as a healthcare service provider.

2. Originally formed as Hospital Corporation of America in 1968, HCA now bills itself as "one of the nation's leading providers of healthcare services" and comprises 182 hospitals

and more than 2,300 sites of care ranging across twenty states—including Tennessee and Florida—and the United Kingdom.[1]

3. As HCA has grown, so too has the amount of data that it collects. HCA boasts that it "[u]ses data from more than 37 million patient encounters each year"—including Plaintiff's and the Class Members' data.[2]

4. To assist patients in providing its services, HCA collects a variety of Sensitive Information, including patients' names, home addresses, email addresses, telephone number, dates of birth, general, and especially sensitive data relevant to patients' treatment such as patients' service dates, location, and next appointment dates.[3] In the wrong hands, these types of sensitive and personally identifying information may be wielded to cause significant harm to the patients whose information was stolen.

5. The U.S. Department of Health and Human Services has instructed that "[i]dentifying information … such as personal names, residential addresses, or phone numbers," although not PHI when listed alone, "would be PHI" and protected by the HIPAA Privacy Rule if it is listed, as here, with "health care provision" data such as service dates and locations.[4]

6. HCA assured patients that it would "maintain appropriate physical, electronic, and procedural safeguards to protect your personal information."[5] Contrary to its representations and promises, however, HCA utilized inadequate data security measures it knew, or should have

[1] https://hcahealthcare.com/about/our-history.dot
[2] https://hcahealthcare.com/about/our-history.dot
[3] https://hcahealthcare.com/about/privacy-update.dot
[4] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html
[5] https://hcahealthcaretoday.com/privacy-policy/

known, put the sensitive data it solicited, collected, and stored at significant risk of theft by or exposure to nefarious parties.

7. Consequently, sometime on or about July 5, 2023, HCA learned that hackers had breached its "external storage location" and obtained the above-listed Sensitive Information that HCA solicited, collected, stored, and had promised to secure (the "Data Breach"). Upon investigation, HCA now states that the breached information comprises approximately 27 million rows of data, including information for approximately 11 million patients.[6]

8. The breached Sensitive Information has already been "made available … on an online forum."[7]

9. More than a week after HCA learned of the breach, on July 14, 2023, HCA publicly acknowledged that patients' data had been breached and began emailing patients to alert them to the Data Breach.[8]

10. HCA has attempted to downplay the Data Breach, claiming that no passwords or payment information had been compromised, and that no "clinical information" had been leaked—despite the fact that patient treatment location and appointment data were compromised. The reality, however, is that the information stolen from HCA is highly valuable and can be used to cause great harm to Plaintiff and the Class Members.

11. The type of information impacted by the Data Breach can be used to orchestrate a host of fraudulent activities, including financial and medical fraud and identity theft. Indeed, a driving purpose of these types of data breaches is to obtain and misuse victims' Sensitive

[6] https://hcahealthcare.com/about/privacy-update.dot
[7] https://hcahealthcare.com/about/privacy-update.dot
[8] https://hcahealthcaretoday.com/privacy-policy

Information or to make it available on the dark web for misuse. Information such as the Sensitive Information accessed during the Data Breach may also be used to fraudulently obtain medical services, or to perform additionally targeted phishing or hacking attacks directed at the victims of the Data Breach. Consequently, all impacted individuals are at a heightened and substantial risk that their information will be disclosed to criminals and misused for attempted or actual fraud or identity theft.

12. Plaintiff Hudson was a patient at one of HCA's facilities and was impacted by the Data Breach. Since the Data Breach, Plaintiff has uncovered evidence of identity theft and financial fraud through her credit monitoring efforts. Around the same time, Plaintiff noticed an increase in fraudulent text messages directed toward her. Plaintiff remains at a continued risk of harm due to the exposure and potential misuse of her personal data by criminal hackers.

13. As such, Plaintiff brings this Complaint on behalf of persons whose Sensitive Information was stolen during the Data Breach.

JURISDICTION

14. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, Plaintiff is diverse from Defendants because Plaintiff is a citizen of Florida and Defendants are both citizens in Tennessee, where they are headquartered, and Delaware, where they are incorporated. Plaintiff alleges that, in the aggregate, the claims of all purported class members exceed $5,000,000, exclusive of interest and costs.

15. This Court has general personal jurisdiction over HCA Inc. and HCA Healthcare, Inc. because both are headquartered and operate their principal places of business in Nashville, Tennessee. Both Defendants have minimum contacts with Tennessee because they are located in and conduct substantial business in Tennessee, and Plaintiff's claims arise from their conduct in Tennessee.

16. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District, and because Defendants conducts a substantial part of their business and are headquartered within this District.

PARTIES

17. **Plaintiff** Angeline Hudson is a citizen of Panama City, Florida. HCA obtained and maintained the Sensitive Information of Plaintiff and owed her a legal duty and obligation to protect and sure that Sensitive Information from unauthorized access or disclosure.

18. Plaintiff Hudson received notice of the Data Breach from HCA via email on July 18, 2023. Plaintiff Hudson suffered actual injury from having her Sensitive Information exposed as a result of the Data Breach, including: (a) time and effort monitoring her accounts for fraudulent charges and to mitigate the risk of harm from the Data Breach; (b) entrusting Sensitive Information to HCA that she would not have had MCA disclosed that it lacked data security practices adequate to safeguard its patients; (c) damages to and diminution in the value of her Sensitive Information—a for of intangible property that she entrusted to HCA as a condition of receiving healthcare services; (d) loss of her privacy; and (e) continuous imminent an impending injury arising form the increased risk of financial, medical, and identity fraud and theft.

19. **Defendant** HCA Inc. is a Delaware corporation with its headquarters and principal place of business at One Park Plaza, Nashville, Tennessee.

20. **Defendant** HCA Healthcare, Inc. is a Delaware corporation with its headquarters and principal place of business at One Park Plaza, Nashville, Tennessee.

FACTUAL ALLEGATIONS

A. HCA Collects Sensitive Information from Users.

21. HCA is a large and experienced healthcare service provider with more than fifty years of experience and locations ranging across twenty states.[9]

22. As a regular part of the services that it provides to patients, HCA maintains patients' highly sensitive personal information. Indeed, to obtain services from HCA, patients, like Plaintiff and the Class, must provide their medical providers with highly sensitive information, including PII, PHI, or both. As a massive healthcare service provider, HCA has collected and maintained an enormous depository of Sensitive Information of millions of patients, which acts as a particularly lucrative, and foreseeable, target for data thieves looking to obtain and misuse or sell patient data.

23. Upon information and belief, through its own privacy policy and through its health care providers, HCA represented to Plaintiff and the Class that their Sensitive Information would be kept confidential and not disclosed to unauthorized third parties.

24. Plaintiff and the Class had a reasonable expectation that HCA would protect the Sensitive Information that it collected and maintained, especially because, given the publicity of other data breaches and the significant impact they had, HCA knew or should have known that failing to adequately protect their information could cause substantial harm.

[9] https://hcahealthcare.com/about/our-history.dot

25. HCA's privacy policies acknowledge the sensitivity of the information that it collects and maintains. HCA agrees that "in both its electronic and physical forms … PII must be protected with administrative, technical, and/or physical safeguards, as appropriate, which it is processed, accessed, stored, or otherwise used.[10]

26. HCA further assures that "[i]f you are one of our patients, your personal information in our possession is protected health information ('PHI') protected by the Health Insurance Portability and Accountability Act of 1996," and that "[j]ust as we strive to protect Personal Information we are committed to protecting your PHI." HCA tells patients that, therefore, "[y]our PHI will remain confidential."[11]

27. As described throughout this Complaint, HCA did not reasonably protect, secure, or store Plaintiff's and the Class's Sensitive Information prior to, during, or after the Data Breach, but rather enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information HCA maintained. Consequently, cybercriminals circumvented HCA's security measures, resulting in a significant data breach.

B. HCA's Inadequate Data Security Measures Exposed Users' Sensitive Data

28. On or before July 5, 2023, malicious actors gained unauthorized access to HCA's systems. According to HCA, the hackers "appear[] to" have gained access to "an external storage location" that is "used to automate the formatting of email messages."[12]

[10] https://hcahealthcare.com/util/forms/ethics/policies/information-protection/IPGEN002-a.pdf
[11] https://hcahealthcaretoday.com/privacy-policy/
[12] https://hcahealthcare.com/about/privacy-update.dot

29. The hackers' access to this Sensitive Information was made possibly by, and caused by, HCA's failure to use reasonable security procedures and practices, especially given the sensitivity of the informaiton that it was maintaining.

30. The precise timing and length of the data breach is not yet known at this time. According to HCA, it did not learn of the data breach until after patients Sensitive Information had already been posted in an online forum on July 5, 2023.[13] It is exceedingly probable, therefore, that Plaintiff's and the Class's Sensitive Information was not only viewed by the cybercriminal, but was further exfiltrated and sold online to other third parties.

31. The Sensitive Information that was accessed an exfiltrated during the Data Breach includes patients' names, home addresses, email addresses, telephone number, dates of birth, general, and especially sensitive data relevant to patients' treatment such as patients' service dates, location, and next appointment dates.[14]

32. Although HCA's lack of vigilance caused the Data Breach, it now states that it is emailing patients to "encourage *them* to be vigilant" regarding their data. HCA has not provided any mitigatory steps for Plaintiff or Class Members to follow to protect their data, however, and instead has merely set up a phone number for patients to call "to ask any general questions."[15]

C. HCA Knew It Needed to Protect Users' Sensitive Data

33. As a healthcare service provider, HCA knew, or should have known, that it needed to implement measures to adequately protect sensitive data. Indeed, HCA consistently represented that it was capable of, and would, protect patients' data.

---

[13] https://hcahealthcare.com/about/privacy-update.dot

[14] https://hcahealthcare.com/about/privacy-update.dot

[15] https://hcahealthcare.com/about/privacy-update.dot (emphasis added).

34. HCA has received ample warning of the need to protect sensitive data.

35. For example, the FTC has issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor data security into all business decision-making.[16] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; using industry tested and accepted security methods; (5) monitoring activity on networks to uncover unapproved activity; (6) verifying that privacy and security features function properly; (7) testing for common vulnerabilities; and (8) updating and patching third-party software.[17]

36. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

37. As such, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access

[16] Federal Trade Comm'n, *Start with Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[17] *Id.*; Federal Trade Comm'n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all proceeded HCA's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

38. HCA was especially on notice of the need to safeguard data because of the history of data breaches in the healthcare industry, which is particularly susceptible to cyber attacks.

39. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 to 2019, the number of healthcare related security incidents increased from 450 annual incidents to more than 570 annually—which is likely

a conservative estimate.[18] By 2021, according to the Verizon Data Breach Investigations Report, the figure had reached 655 known data breaches.[19]

40. As a healthcare service provider ranging across twenty states and serving millions of patients, HCA knew or should have known the importance of protecting the Sensitive Information entrusted to it. HCA also knew or should have known of the foreseeable and catastrophic consequences if its systems were breached. Despite this, HCA failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

41. HCA could have minimized or altogether prevented the Data Breach by taking reasonable steps to properly secure and encrypt the Sensitive Information of Plaintiff and the Class and by maintaining a reasonable information retention policy to delete unnecessary patient information.

D. HCA's Data Breach Harmed Plaintiff and the Class

42. Plaintiff's and the Class's data exposed in the Data Breach constitute the type of data specifically targeted by and valuable to hackers.

[18] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats (last visited July 31, 2023).

[19] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/ (last visited July 31, 2023).

43. Indeed, hackers increasingly sell these sensitive records on the black market to purchasers who seek to use the personally identifying information to create fake IDs, make fraudulent transactions, obtain loans, or commit other acts of identity theft.[20]

44. The risk of identity theft after a data breach is lasting. The U.S. Government Accountability Office's research into the effects of data breaches found that "in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web—as is the case in this Data Breach—fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot rule out the significant risk of future harm."[21]

E. Plaintiff's Experience

45. As a condition of receiving health care, Plaintiff Hudson provided HCA with her highly personal information, including PII and PHI as described in the foregoing paragraphs. HCA maintained access to and control over this Sensitive Information. Plaintiff Hudson expected that her Sensitive Information would remain safeguarded and would not be accessible by unauthorized third parties.

46. However, on July 18, 2023, Plaintiff Hudson received notice from HCA that HCA's patients' data had been breached.

---

[20] *How do hackers make money from your stolen data?*, Emsisoft.com (Feb. 20, 2020), https://blog.emsisoft.com/en/35541/how-do-hackers-make-money-from-your-stolen-data/

[21] Report to Congressional Requesters, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown 29 (Jun. 2007), http://www.gao.gov/new.items/d07737.pdf (last accessed Nov. 30, 2018).

47. Subsequent to and as a direct result of the Data Breach, Plaintiff Hudson began receiving fraudulent text messages asking her to enter one-time passcodes, when she had never requested such one-time passcodes.

48. Also subsequent to and as a direct and proximate result of the Data Breach, Plaintiff Hudson has uncovered four fraudulent social security numbers, addresses, and names on her Experian credit report.[22] Plaintiff Hudson has diligently monitored her credit for years, and prior to the Data Breach had never uncovered any fraudulent activity on her report. Plaintiff now finds it necessary to monitor her credit through additional credit agencies in addition to Experian in order to counter the fraudulent activity occurring due to the Data Breach.

49. Plaintiff Hudson is very careful about sharing and protecting Sensitive Information. Plaintiff has never knowingly transmitted unencrypted Sensitive Information over the internet or any other unsecured channel.

50. Plaintiff Hudson suffered actual injury from having her sensitive information exposed and/or stolen as a result of the Data Breach, including but not limited to: (a) mitigation efforts, including monitoring of Plaintiff's credit and account and other efforts to ensure that her information is not being used for financial, medical, and identity theft or fraud, and time and expense thereof; (b) damages to and diminution of the value of her Sensitive Information, a form of intangible property that loses value when it falls into the hands of criminals who are using that informaiton for fraud or publishing the information for sale on the dark web; (c) loss of privacy;

[22] Plaintiff Hudson monitors her credit through Experian monitoring made available through her bank, not through any credit monitoring that HCA has made available. In fact, to date HCA has not made any credit monitoring available to Plaintiff.

(d) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft.

51. In addition, knowing that hackers accessed her Sensitive Information and that this will likely has been and/or will be used in the future for financial, medical, and identity theft has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

52. Despite HCA's failure to reasonably protect Plaintiff's and the Class's Sensitive Information, it has not offered any compensation or adequate remedy, especially considering the significant and long-term risk Plaintiff and the Class face.

CLASS ALLEGATIONS

53. Plaintiff brings this action on behalf of himself and all other persons similarly situated pursuant to Fed. R. Civ. P. 23 and seeks certification of the following Nationwide Class:

> All individuals that received or were otherwise sent notice that their data was potentially compromised due to HCA's Data Breach.

54. Excluded from the class is HCA and its subsidiaries and affiliates; all employees of HCA; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

55. Plaintiff reserves the right to, after conducting discovery, modify, expand or amend the above Class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

56. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are hundreds of thousands of members of the Class. The number of reportedly impacted individuals already exceeds 100,000, and Plaintiff believes additional entities and

persons may have been affected by the Data Breach. The precise number of class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

57. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether HCA knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;

b. Whether HCA controlled and took responsibility for protecting Plaintiff's and the Class's data when solicited that data, collected it, and stored it on its servers;

c. Whether HCA's security measures were reasonable in light of the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether HCA owed Plaintiff and the Class a duty to implement reasonable security measures;

e. Whether HCA's failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether HCA's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of HCA's failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to relief.

58. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the Class are each persons whose provided data to HCA, whose data resided on HCA's servers, and whose personally identifying information was exposed in HCA's Data Breach. Plaintiff's injuries are similar to other class members and Plaintiff seeks relief consistent with the relief due to the Class.

59. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against HCA to obtain relief for himself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

60. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

61. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), HCA, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

LEGAL CLAIMS

COUNT I
Negligence

62. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

63. HCA owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class, and managed and stored. This duty arises from multiple sources.

64. HCA owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target HCA's data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. HCA alone controlled its technology, infrastructure, and cybersecurity. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, HCA knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of HCA's unsecured, unreasonable data security measures.

65. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required HCA to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of HCA's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like HCA of failing to use reasonable measures to protect sensitive data. HCA, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of HCA's duty to adequately protect sensitive information. By failing to implement reasonable data security measures, HCA acted in violation of § 5 of the FTCA.

66. HCA is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring HCA to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

67. Finally, HCA assumed the duty to protect users' sensitive data by soliciting, collecting, and storing users' data and, additionally, by representing to consumers that it would keep their data safe.

68. HCA breached its duty to Plaintiff and the Class by implementing unreasonable data security measures that it knew or should have known could cause a Data Breach. As a self-proclaimed technology "Vanguard", HCA knew or should have known that hackers might target sensitive data that HCA solicited and collected on its users and, therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed, HCA acknowledged it was subject to certain standards to protect cardholder data and password information and utilize other industry

standard data security measures. HCA, furthermore, represented to users that their data was safe with HCA.

69. HCA was fully capable of preventing the Data Breach. HCA, as a smart technology expert, knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. HCA thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

70. As a direct and proximate result of HCA's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

COUNT II
Negligence *Per Se*

71. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

72. HCA's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which HCA failed to do.

73. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by

businesses like HCA of failing to use reasonable measures to protect users' sensitive data. The FTC publications and orders described above also form the basis of HCA's duty.[23]

74. HCA violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. HCA's conduct was particularly unreasonable given the sensitive nature and amount of data it stored on its users and the foreseeable consequences of a Data Breach should HCA fail to secure its systems.

75. HCA's violation of Section 5 of the FTC Act constitutes negligence per se.

76. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

77. As a direct and proximate result of HCA's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III
Declaratory and Injunctive Relief

78. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

79. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

[23] *See supra*, note 75 (listing orders).

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

80. An actual controversy has arisen in the wake of the Data Breach at issue regarding HCA's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges HCA's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

81. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. HCA owed, and continues to owe a legal duty to secure the sensitive information with which it is entrusted, specifically including patients' personal and health information, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. HCA breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal information; and,

c. HCA's breach of its legal duty continues to cause harm to Plaintiff and the Class.

82. The Court should also issue corresponding injunctive relief requiring HCA to employ adequate security protocols consistent with industry standards to protect its users' (*i.e.* Plaintiff's and the Class's) data.

83. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of HCA's data systems. If another breach of HCA's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

84. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to HCA if an injunction is issued.

85. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

86. Wherefore, Plaintiff, on behalf of himself and the Class, requests that this Court award relief as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and their counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. An award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

87. Plaintiff hereby demands a jury trial for all the claims so triable.

Dated: August 1, 2023

Respectfully submitted,

/s/ J. Gerard Stranch, IV

J. Gerard Stranch, IV (TN Bar No. #23045)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com

Brian C. Gudmundson (*pro hac vice forthcoming*)
Charles R. Toomajian III (*pro hac vice forthcoming)*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
charles.toomajian@zimmreed.com